# 发展网络空间可视化技术 支撑网络安全综合防控体系建设

郭启全[1,2] 高春东[1] 郝蒙蒙[1*] 江 东[1]
1 中国科学院地理科学与资源研究所 北京 100101
2 中华人民共和国公安部 网络安全保卫局 北京 100741

**摘要** 网络安全是信息化时代国家安全的基石，网络空间可视化表达是网络安全综合防控的重要基础。文章基于“人-地-网”纽带关系理论，提出了网络空间可视化表达的内涵及技术路径，对网络空间要素、网络空间关系、网络安全事件的可视化进行了描述与分析。以网络空间地理学为基础对网络空间可视化技术的探索与应用，作为构建网络空间与现实空间映射关系、绘制网络空间地图的重要内容，将为实现网络安全综合防控建设和“挂图作战”提供有力支撑。

**关键词** 人地网关系，网络空间地图，网络空间，地理空间，可视化表达

DOI 10.16418/j.issn.1000-3045.20200302004



随着全球信息化的快速发展，人类对网络空间的依赖程度越来越高，网络空间成为世界各国竞争博弈的新领地，网络空间安全已成为一个国家存在与发展的重要保障[1,2]。习近平总书记明确指出，没有网络安全就没有国家安全。在传统的地理空间，地图作为描绘地理现象的重要载体，自古以来就是指挥作战不可或缺的工具；如今在网络空间，也迫切需要能够全面展示网络空间信息的网络空间地图[3,4]，从而建立起网络空间与地理空间的关联。依托网络安全态势感知平台，将网络空间地图与平台智慧大脑有机结合，实现网络空间的“挂图作战”。

网络空间地图不仅对网络安全职能部门、行业管理部门、网络运营者、互联网企业等部门和机构有着巨大帮助，也是对涉网国际政治法律和涉网国内经济、政治、文化、法治的有力支撑。绘制网络空间地图，就是要实现对网络空间的可视化表达，这是认识和理解网络空间的重要基础。网络空间地理学（Cyberspace Geography）的提出为绘制网络空间地图

*通讯作者
修改稿收到日期：2020年7月2日

提供了理论支撑[1,2]。在“人-地-网”纽带关系理论基础上，推进对网络空间可视化技术的探索与应用，是绘制实时、可靠、有效的网络空间地图的重要内容，有助于对网络空间的科学认知及网络安全综合防控体系建设。

## 1 网络空间可视化表达发展现状

网络空间资源测绘是目前网络空间可视化表达比较成熟的技术，它能对网络空间中的各类资源及其属性进行探测、融合分析和绘制[5,6]。代表性工作包括美国国防部高级研究计划局的“X 计划”[7]、美国国土安全部的“SHINE 计划”[8]、美国国家安全局的“藏宝图计划”①。此外，美国诺思公司（Norse）②、俄罗斯卡巴斯基实验室（Kaspersky）③等机构通过收集网络攻击数据，绘制了网络威胁实时地图。某研究机构设计研发的“网络资产测绘分析系统——网探 D01”初步实现了网络空间资产测绘；某安全企业基于“钟馗之眼”（Zoomeye）④探测的网络基础设施，绘制了全球 42 亿 IP 地址的网络空间地图。虽然网络空间测绘实现了对网络空间主要要素的探测与展示，但并未全面展示网络空间，仅是对网络空间进行了局部信息的可视化。

Martin 和 Rob[9,10]对网络空间可视化进行了较为深入的研究，代表性成果是 *The Atlas of Cyberspace* 和 *Mapping Cyberspace* 2 本著作。前者选取了网络空间的 4 个不同对象（网络基础设置与流量，万维网，在线会话与社区，以及艺术、文学和电影），绘制了不同对象下的网络空间地图；后者则在前期研究的基础上，提出了一种理解网络空间面貌的认知方式，尝试从空间性、空间形态和时空关系的角度绘制了部分网络地图，并分析了网络空间与地理空间之间的关联性和互动性。这些工作是展现网络空间面貌的有益探索，但仍停留在比较初级的层次，难以描绘网络空间全貌，也并未真正意义上实现网络空间可视化表达。此外，由于对网络安全信息进行结构化组织与聚合的呈现能力不足，目前的成果不足以支撑分析者有效制定决策并开展响应行动，不能充分满足网络空间安全防控的实际应用需求。

## 2 网络空间可视化表达的发展动力与支撑

目前，网络空间可视化表达研究尚处于起步阶段，其发展需要以业务部门的应用需求为导向，以成熟的理论体系和技术基础为支撑。

### 2.1 业务部门的应用需求是网络空间可视化表达发展的驱动力

网络安全传统的业务工作多是以文本、图表等方式进行查询与显示。由于网络空间信息量大、种类繁多、表现形式复杂，而传统的工作形式忽略了网络空间与地理空间的映射关系，无法直观表现网络空间信息的多维特性，难以多角度、全方位地提供清晰明确的信息支持。只有对地理、资产、事件、情报等大数据进行融合分析，再加上可视化呈现技术，网络安全工作才能更智能化、自动化、可视化。

除了支撑网络安全业务之外，网络空间可视化表达也是国际关系、国际法、区域法等涉网国际政治法律问题的基础和支撑，是资源、产权、监管、司法等涉网国内经济、政治、文化、法治的基础和保障，也是国家治理体系和治理能力现代化在网络空间中进行建设和实施的基本要素和重要保障。各类业务的迫切需求是网络空间可视化表达发展的驱动因素，亦为网

① Grant T. On the military geography of cyberspace. Proceedings, 9th International Conference on Cyber Warfare & Security (ICCWS 2014). 2014: 66-76.

② http://norsenet.com.

③ https://cybermap.kaspersky.com.

④ https://www.zoomeye.org.

络空间可视化表达提供了信息支撑与方向指导。不断拓展网络空间可视化表达的应用领域，将是下一步需要探索的重要工作之一。

### 2.2 成熟的理论体系和技术方法是网络空间可视化表达的基础

任何一个新兴学科的发展都需要成熟的理论体系和技术方法。最初，国外学者提出把网络空间看作一个虚拟现实世界，应具有地理空间相应的位置属性和坐标表达[11]。随着网络空间虚拟化特征越来越显著，动态网络拓扑图被认为是可以反映网络空间信息关系的一种表达方式⑤。在科学技术快速发展的推动下，基于地理学、图形学、计算机通信、信息可视化等理论基础，网络空间的社区、地图和映射的理论被提出，通过学科与技术交叉，建立了网络空间可视化的基本方法⑥。2010 年以来，我国学者引入地图思想，并对网络空间表达进行了大量的探索。参考地图的表达方式，我国学者提出网络空间亦可制定规范的符号系统，用以表达网络空间的各类要素及信息变化[12,13]。同时，借鉴地图中的栅格数据形式，将网络空间根据不同的属性划分为物理网格、逻辑网格和社会域网格；并根据不同的网格形态，探索了其内涵及表达方式[14]。以地图模型为启发，我国学者还提出了网络空间地图模型构建体系，其涵盖网络空间要素符号体系、多尺度表达方式及应用分析[15,16]。总的来看，上述网络空间可视化表达理论较为零散，且都是概念性的、没有形成成熟的理论体系和技术方法。

结合前期不同学者的相关研究，高春东等[1,2]将地理学的思想引入到网络空间，首次提出“网络空间地理学”的概念，系统梳理了网络空间地理学的理论基础、研究内容和技术路径，并明确提出网络空间可视化表达是网络空间地理学研究的主要内容之一。“网络空间地理学”的构建在一定程度上解决了网络空间可视化表达理论基础和技术方法薄弱的问题。

## 3 网络空间可视化表达的主要内容及技术路径

地理学中完善的系统理论和地图学的成熟思想，为绘制网络空间地图提供了非常好的参考准则。“人-地”关系理论是地理学研究的核心内容，随着信息化的迅猛发展，人与人之间地理空间的限制被打破，“人-地-网”新型纽带关系逐渐建立[3,4]。在“人-地-网”关系的相互作用与融合下，将地理学的理论方法引入网络空间，为实现网络空间可视化表达提供了新思路。网络空间可视化表达主要包括网络空间要素可视化表达、网络空间关系可视化描述和网络安全事件可视化分析等（图 1）。

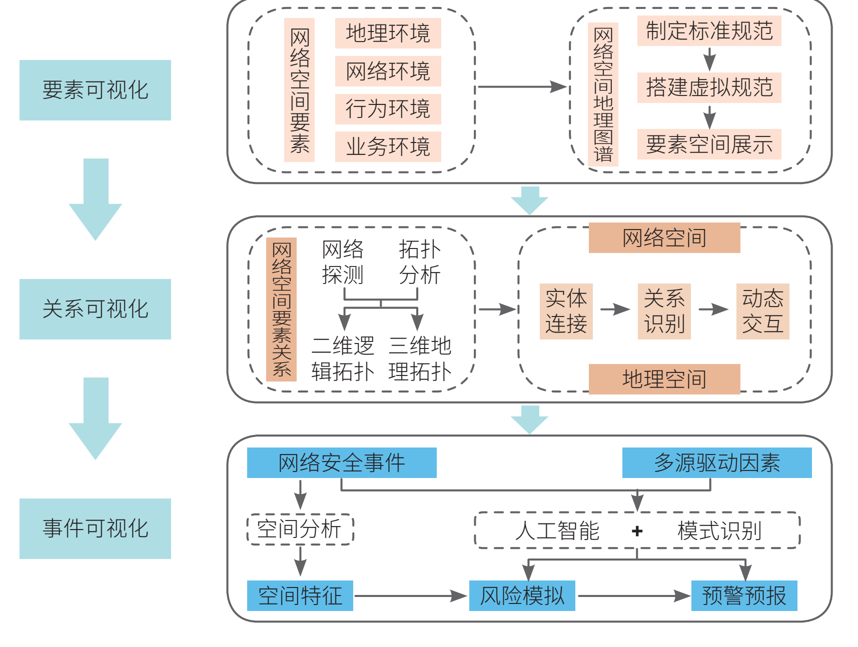



图 1　网络空间可视化表达的内涵与技术路径

⑤ http://pdfs.semanticscholar.org/1bd3/0afd5b67239588fd363a4fc01ef4d9e5a097.pdf.
⑥ Smith M A, Drucker S M, Kraut R E, et al. Counting on community in cyberspace. Conference: CHI’99 extended abstracts, 1999.

网络空间具有高度的复杂性，并与地理空间高度关联，共同构成了人类活动的现实空间。要绘制一组能够实时、动态、真实反应网络空间并将其与地理空间统一融合的网络空间地图，需要多种技术相融合。① 以地理空间可视化为基础，融入网络安全事件和网络空间资产数据，从地理、资产、事件维度丰富可视化表达，全面展示和描述网络空间资源的分布和属性，实现网络空间要素的可视化表达。② 在网络空间要素表达基础上，探讨社会人、网络、地理空间与数字化信息数据间的相互关联和影响，将网络拓扑关系映射到地理空间，实现网络关系的可视化。③ 以事件为触发条件，通过图形快速串联事件、资产和地理要素，明晰各要素之间的互动关系，形成一组动态、实时、可靠、有效的网络空间作战指挥地图，使资产底数更加清楚、事件发现更加精确、威胁定位更加准确、威胁分析更加智能、威胁溯源更加自动；提高业务部门在事件发现、取证定位、追踪溯源方面的能力和效率，使职能部门工作更加智能化、自动化、可视化。

地理环境
- 基础地理信息
- 公共地理信息
- 影像及三维模型

网络环境
- 物理环境
- 逻辑环境

行为主体
- 实体角色
- 虚拟角色

业务环境
- 网络事件
- 网络服务主体
- 关键信息基础设施

网络空间

地理环境 网络环境 行为主体 业务环境

图 2　网络空间要素构成

## 3.1 网络空间要素可视化表达

### 3.1.1 网络空间要素体系

网络空间要素可视化表达是网络空间可视化表达的基础，但当前尚未形成较为系统的网络空间要素分类体系。传统的网络空间要素仅根据网络空间的物质属性和社会属性进行分类，忽视了网络空间要素的地理属性。在“人-地-网”纽带关系理论指导下，网络空间要素分类应从网络空间拓展到网络-地理空间。根据网络空间要素自身的结构和特点，并结合网络安全业务需求，本文将网络空间要素划分为地理环境、网络环境、行为主体和业务环境 4 个层次（图 2）。

① 地理环境层。它是各类网络空间要素依附的载体，强调网络空间要素的地理属性，如网络基础设施和网络行为主体的地理位置、空间分布和区域特性，涉及距离、尺度、区域、边界、空间映射等概念。② 网络环境层。主要是各类网络空间要素形成的节点和链路，即逻辑拓扑关系，又可分为物理环境和逻辑环境，包含各种网络设备、网络应用、软件、数据、IP、协议等。③ 行为主体层。包含实体角色和虚拟角色，关注网络行为主体（即实体角色或虚拟角色）的交互行为及其社会关系，包括信息流动、虚拟社区、公共活动空间等。④ 业务环境层。主要包括业务部门重点关注的各类网络安全事件（案件）、网络安全服务主体、网络安全保护对象等。地理环境层、网络环境层、行为主体层和业务环境层 4 个层次的要素之间相互联系、相互影响，共同构成网络空间要素体系。

### 3.1.2 可视化表达方法

网络空间要素可视化表达主要分析网络空间要素的类型、层次、时空基准、表达标准和尺度问题，并以网络空间地理图谱的形式进行展示。网络空间要素表达以网络空间地理测绘及地图构建为基础，将地理空间中

网络地理实体抽象成为多尺度的空间对象，利用网络探测成果与网络拓扑结构数据，结合空间链接与实体映射，构建网络空间地图。① 基于网络空间关键要素指标体系，构建网络空间地理图谱建设的数据标准和制图规范；② 通过地理编码、实体测绘和建筑信息模型（BIM）软件建模等手段，将地理环境和网络实体进行空间化，实现虚拟地理环境的三维场景建模；③ 通过网络资产探测，全面获取网络资源情况及相应的安全事件，将网络空间要素映射至地理空间，以地理信息图、逻辑图和拓扑图的形式绘制网络空间基础设施和网络资产地图；④ 通过若干图层的分层展示，全面直观地描述网络空间要素在网络空间的时空分布及其属性状态和变化情况，形成一组动态、实时、可靠、有效的网络空间要素图。

### 3.2 网络空间关系可视化描述

网络空间关系可视化描述主要包括网络要素之间的关系，以及网络空间与地理空间之间的关系。网络空间关系可视化主要研究网络空间的结构特性，并结合网络空间和地理空间要素的交互映射，研究网络空间和地理空间的多尺度拓扑关联，实现网络实体在网络空间、地理空间的结构投影。

网络要素之间的关系通过网络探测和拓扑分析技术，分析网络资源属性，形成内容丰富的网络实体连接拓扑结构，实现不同级别不同颗粒度的网络拓扑可视化，展示各类范围的拓扑关系，包含全球、国家间、国家内、AS[⑦]域间、AS 域内的三维地理拓扑和二维逻辑拓扑等。地理空间和网络空间具有复杂的耦合关联关系，网络空间与地理空间之间的关系可视化重点是实现 2 个空间的动态交互。结合网络空间要素可视化，基于网络资产探测、网络拓扑空间化、二维和三维一体化网络地理数据关联等技术，研究多尺度地理空间和网络空间的实体连接和关系识别，探索空间、信息与人类行为之间的内在关联，实现地理空间与网络空间的多尺度、多维度、动态可视化。

以城市尺度综合展示网络拓扑各节点间关系，以及网络空间与地理空间之间的关系为例（图 3），城市网络要素关系常以二维逻辑拓扑的形式进行展示，可视化程度较差。依据网络拓扑结构中的核心层、汇

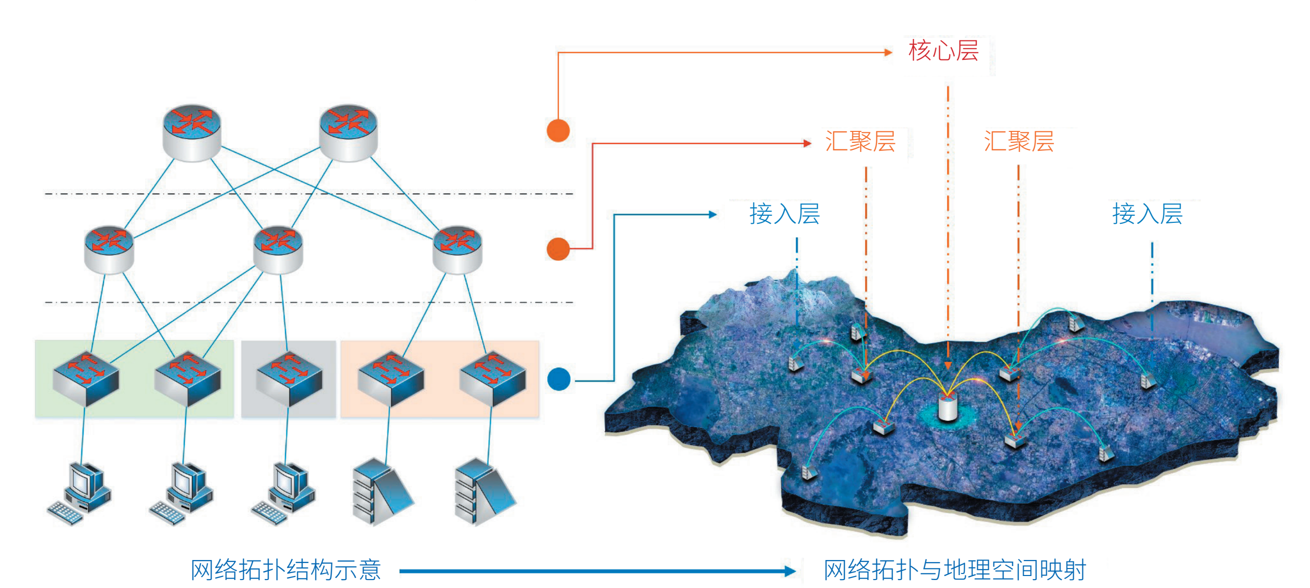



图 3 网络空间关系描述示意

按照网络分级设计模型，通常把网络设计分为核心层、汇聚层和接入层，各层之间的关系以拓扑的形式进行展示（图左）；为了增加可视化效果，确定各层次关键节点的地理位置，在地理空间中表达各层次之间的关系（图右）

⑦ AS（autonomous system），互联网自治系统。全球的互联网被分成 65 536 个 AS 域。

聚层和接入层各节点关系，结合城市二维与三维地理要素位置分层展示，每个节点都与地图上的地理实体相关联。通过网络拓扑图的分层展示，既为网络空间关系提供了较清晰的可视化效果，又与地理空间建立了充分的联系。

### 3.3 网络安全事件可视化分析

网络安全事件（含案件）可视化分析是指将复杂、动态的网络安全事件按照行为主体、客体和影响等，分析网络安全事件发生的驱动因素及内部机理，实现网络安全事件的态势感知和预警预报，并在网络空间地图上进行画像和过程展示。

网络安全事件可视化分析以具有地理信息特征的海量网络安全事件为基础，通过资源化整合，将网络大数据转化为网络安全事件信息资源，并借鉴地理学空间分析方法与技术，对网络安全事件的时空分布特征和网络集聚特征进行分析展示。针对某一类网络安全事件，综合考虑该类事件的物质属性、社会属性和地理属性，获取与该类事件相关的网络空间要素集，在空间尺度上以该类事件为主体，以相关的网络空间要素集为该类事件的特征向量，采用机器学习算法对该类网络安全事件风险进行模拟分析，预测该类事件的风险分布。业务部门在此基础上，可采用深度学习和模式识别对该类事件的发展态势进行预警预报，提升对该类事件的发现和处置能力，实现此类网络安全事件的“早发现、早预警、早处置”。

以网络安全事件中的攻击事件为例，首先根据哨点探针、威胁情报和相关数据，同时与历史数据进行匹配，分析该攻击事件的特征并对攻击事件进行溯源（图4）。通过实体定位技术确定发起攻击的位置及跳板位置，并在地图上以不同的颜色、宽度和方向表示当前攻击的方法、类型和方向，辅助工作人员对当前攻击事件快速了解和及时处置。此外，及时将该攻击事件收录至网络安全事件数据库中，作为之后攻击事件分析的本底数据。而对于网络安全事件中的漏洞发现情报，则可借助重点保护单位建筑三维建模工作，快速定位至漏洞出现的空间位置。结合漏洞通报事件处置流程，快速将漏洞信息和发现漏洞的实体空间位置精确通报给涉事单位联系人，实现漏洞的快速处置，以在地图的不同尺

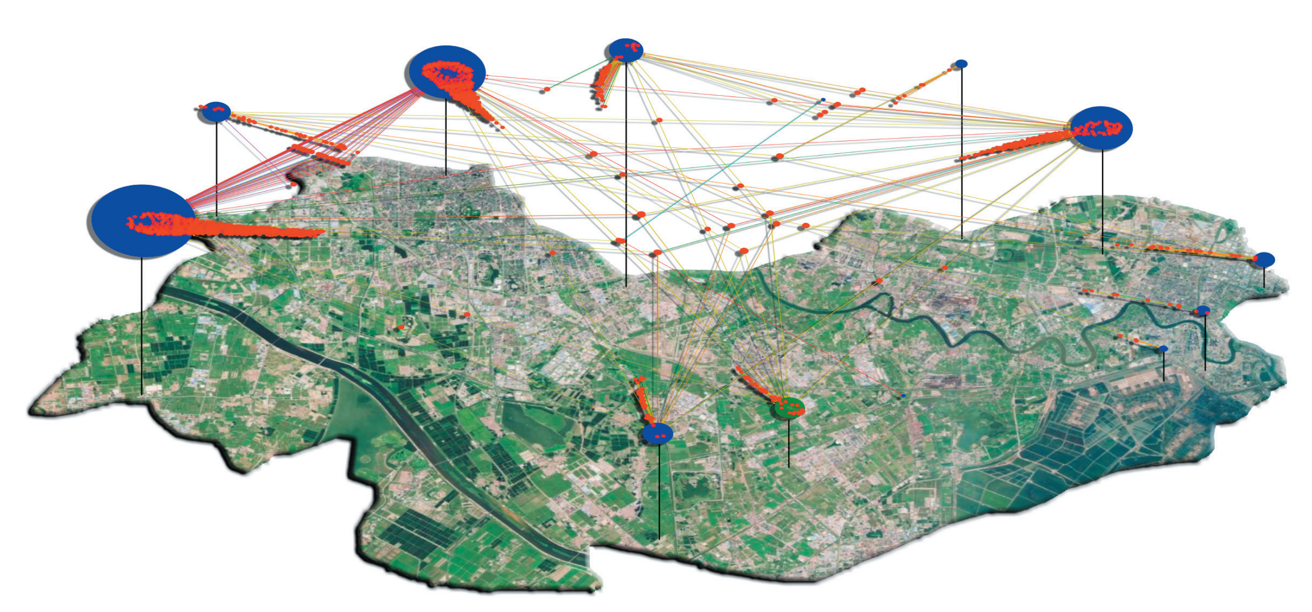


图4　网络攻击事件可视化示例

在地理空间中表示攻击事件，通过实体定位技术确定攻击者和被攻击节点的地理位置，并将被攻击节点的位置定位到二、三维地图上，以节点颜色表示节点类型，节点大小表示节点重要程度，以连线表示攻击路径，线的颜色表示不同攻击类型，线宽表示攻击频次

度上服务于业务部门工作需求。

总之，网络安全事件可视化分析通过空间图、网络图的形式集中表达网络安全事件分析的全过程；结合人工智能和大数据分析技术，对攻击事件及攻击者、攻击手段等进行画像；对网络空间要素、模型运算和应急处置进行全生命周期的场景展示。当应用于网络攻击实时监控、网络安全事件追踪溯源、网络安全态势感知、通报预警、应急处置、侦查打击、指挥调度等典型业务场景时，可使业务部门的工作更加智能化、自动化、可视化。

## 4 思考及讨论

网络空间可视化表达的终极目标在于以网络空间地图的形式全面展示网络信息，实现网络空间的具象化与数字化，从而为决策者提供直观、有价值的信息，以降低决策的不确定性。网络空间可视化表达应以地理空间可视化为样本，融入网络空间要素和网络安全事件，从要素、关系、事件等维度丰富可视化表达内容，绘制网络空间地图，实现网络空间各类事件全过程一组图串联展示，服务公安机关的“挂图作战”，提升网络空间监测预警能力。

网络空间可视化表达的发展前期面临理论基础薄弱、技术不成熟等问题，网络空间地理学理论体系与技术方法的提出为网络空间可视化研究提供了新视角。网络空间可视化表达的实现涉及地理学、信息技术、大数据、人工智能等诸多学科领域，因此需要多方面协同、多学科交叉融合来满足网络空间可视化表达的业务应用需求，共同促进网络安全综合防控体系建设。

## 参考文献


1 高春东, 郭启全, 江东, 等. 网络空间地理学的理论基础与技术路径. 地理学报, 2019, 74(9): 1710-1722.

2 Gao C, Guo Q, Jiang D, et al. Theoretical basis and technical methods of cyberspace geography. Journal of Geographical Sciences, 2019, 29(12): 1949-1964.

3 孟威. 网络安全: 国家战略与国际治理. 当代世界, 2014, (2): 46-49.

4 赵帆, 罗向阳, 刘粉林. 网络空间测绘技术研究. 网络与信息安全学报, 2016, 2(9): 1-11.

5 金伟新. 网络空间面临的战争威胁和应对策略. 中国信息安全, 2015(11): 113-115.

6 郭莉, 曹亚男, 苏马婧, 等. 网络空间资源测绘: 概念与技术. 信息安全学报, 2018, 3(4): 1-14.

7 Nakashima E. With Plan X, Pentagon seeks to spread US military might to cyberspace. The Washington Post, 2020-05-31.

8 Müller-Maguhn A, Poitras L, Rosenbach M, et al. Treasure map: The NSA breach of telekom and other German firms. Spiegel Online, 2012-04-16.

9 Dodge M, Kitchin R. The Atlas of Cyberspace. Massachusetts: Addison-Wesley Reading, 2001.

10 Dodge M, Kitchin R. Mapping Cyberspace. London: Routledge, 2003.

11 Benedikt M. Cyberspace: First Steps. Massachusetts: MIT Press, 1991

12 张峥. 赛博地图构建理论研究. 郑州: 中国人民解放军战略支援部队信息工程大学, 2012.

13 艾廷华, 周梦杰, 陈亚婕. 专题地图属性信息的LOD表达与TreeMap可视化. 测绘学报, 2013, 42(3): 453-460.

14 蒋秉川, 万刚, 徐锐. 网络空间剖分机理与可视化方法研究. 系统仿真学报, 2017, 29(S1): 1-8.

15 张龙, 周杨, 施群山, 等. 与地理空间紧关联的网络空间地图模型. 信息安全学报, 2018, 3(4): 63-72.

16 张龙, 周杨, 田江鹏, 等. 语义驱动下的网络资源符号设计方法. 计算机科学. 2019, 46(4): 83-88.

# Develop Visualization Technology of Cyberspace to Support Construction of Comprehensive Prevention and Control System of Cyber Security

GUO Qiquan[1,2] GAO Chundong[1] HAO Mengmeng[1*] JIANG Dong[1]

( 1 Institute of Geographic Sciences and Natural Resources Research, Chinese Academy of Sciences, Beijing 100101, China;

2 Cyber Security Department, The Ministry of Public Security of the People's Republic of China, Beijing 100741, China )

**Abstract** Cyber security is the basis of national security in the information age, and the visualization of cyberspace is of vital importance for comprehensive prevention and control of cyber security. Based on the theory of "man-land-network" nexus, this study proposed the connotation and technical path of cyberspace visualization and described the visualization of the cyberspace elements, cyberspace relations, and cyberspace security events. Based on the cyberspace geography, the exploration and application of cyberspace visualization technology is an important content of constructing the mapping relations between cyberspace and real world as well as drawing a cyberspace map, which will provide a significant support for the realization of the cyberspace map in the comprehensive prevention and control of cyber security.

**Keywords** man-land-network relationship, cyberspace map, cyberspace, geographical space, visualization



**郭启全** 公安部网络安全保卫局一级巡视员、副局长、总工程师，中国科学院地理科学与资源研究所特聘研究员。主要从事网络空间安全、网络空间地理学等方面的研究。E-mail: xxaqgc@163.com

**GUO Qiquan** Inspector, Deputy Director and Chief Engineer of the Cyber Security Department, the Ministry of Public Security (PRC). The distinguished researcher of Institute of Geographic Sciences and Natural Resources Research, Chinese Academy of Sciences. His research focuses on national cyberspace security. E-mail: xxaqgc@163.com



**郝蒙蒙** 中国科学院地理科学与资源研究所助理研究员。主要从事网络空间地理学、地理信息系统等方面的研究。E-mail: haomm@igsnrr.ac.cn

**HAO Mengmeng** Assistant Researcher of Institute of Geographic Sciences and Natural Resources Research, Chinese Academy of Sciences. Her research focuses on cyberspace geography, geographic information system, etc. E-mail: haomm@igsnrr.ac.cn

■责任编辑：文彦杰

* Corresponding author